IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

RONALD J. PANNOZZI, PAOLA BALDOMAR, MEREDITH BRANDT, MONICA DEPINA, MEGHAN KONOPKA, JOAN RATCLIFFE, and RENEE TRIGUEIRO, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

DELOITTE CONSULTING LLP,

Defendant.

CASE NO. 1:24-cv-00524-MRD-LDA

CONSOLIDATED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Ronald J. Pannozzi, Paola Baldomar, Meredith Brandt, Monica Depina, Meghan Konopka, Joan Ratcliffe, and Renee Trigueiro ("Plaintiffs") bring this action individually and on behalf of all others similarly situated against Defendant Deloitte Consulting LLP ("Deloitte" or "Defendant"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from Deloitte. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises from Deloitte's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs' and Class Members' highly sensitive personal information, which it acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack that purportedly occurred in December of 2024 and compromised Defendant's network (the "Data Breach" or

"Breach") containing personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of Plaintiffs and other individuals. Upon information and belief, cyber-criminals hacked into the systems of Defendant and obtained Private Information for over 700,000 Rhode Island residents, including, but not limited to: Plaintiffs' and Class Members' names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, driver's license or state ID information, passport information, financial information, health information, usernames and passwords, biometric information, gender/sexual orientation information, and signatures.

3. The Data Breach involved documents and information stored on the computer network of Deloitte on behalf of RIBridges, a large government entity that administers state benefits. Deloitte assists in business operations for RIBridges.

4. On its computer network, Deloitte holds and stores certain highly sensitive Private Information of Plaintiffs and the putative Class Members, who are individuals who applied for or are enrolled in state benefits administered by RIBridges. In other words, Plaintiffs and the putative Class Members are individuals who provided their highly sensitive Private Information in exchange for state benefits and services.

5. The programs and benefits affected by this Breach include:

- Medicaid
- Supplemental Nutrition Assistance Program (SNAP)
- Temporary Assistance for Needy Families (TANF)
- Child Care Assistance Program (CCAP)
- Health insurance coverage purchased through HealthSource RI
- Rhode Island Works (RIW)
- Long-Term Services and Supports (LTSS)
- General Public Assistance (GPA) Program

6. Deloitte admitted and concluded that "that there had been a breach of the RIBridges system based on a screenshot of file folders sent by the hacker to Deloitte" and that the files also

contained "personal identifiable data from RIBridges."[1]

7. Defendant launched an investigation into the Data Breach and confirmed that an unauthorized actor accessed its system in December of 2024 and may have copied and exfiltrated certain files containing Plaintiffs' and Class Members' Private Information.

8. Despite learning of the Data Breach on or about December 5, 2024 and determining that Private Information was exposed in the Breach, Defendant did not begin sending notices of the Data Breach until January 10, 2025 (the "Notice of Data Breach Letter" or "Notice").[2]

9. As a result of Deloitte's Data Breach, Plaintiffs and hundreds of thousands of Class Members suffered ascertainable losses in the form of financial losses from identity theft, out-of-pocket expenses, loss of the benefit of their bargain, and the lost value of their time reasonably incurred to remedy or mitigate the effects of the Breach.

10. Plaintiffs' and Class Members' highly sensitive Private Information—which was entrusted to Defendant, who claims that it uses "a range of physical, electronic and managerial measures to keep your Personal Information secure, accurate and up to date"[3]—was compromised and unlawfully accessed and extracted during the Data Breach.

11. Based upon Deloitte's notice to RIBridges, the Private Information compromised in the Data Breach was intentionally accessed, removed, and exfiltrated by the cyber-criminals who perpetrated this attack and remains in the hands of those same cyber-criminals.

---

[1] *Governor McKee Issues Update on Cybersecurity Breach of RIBridges System*, State of Rhode Island Newsroom (Dec. 14, 2024), https://governor.ri.gov/press-releases/governor-mckee-issues-update-cybersecurity-breach-ribridges-system.

[2] *RIBridges Alert*, State of Rhode Island, Dep't of Administration, https://admin.ri.gov/ribridges-alert (last visited Mar. 27, 2025).

[3] *Privacy Notice*, Deloitte, https://www.deloitte.com/global/en/legal/privacy.html?icid=bn_privacy (last visited Mar. 27, 2025).

12. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

13. Plaintiffs bring this class action lawsuit individually and on behalf of those similarly situated to address Defendant's failure to adequately secure and safeguard Class Members' Private Information and failure to provide timely and adequate notice to Plaintiffs and Class Members of the Breach.

14. Defendant stored and maintained Plaintiffs' and Class Members' Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

15. Defendant disregarded the privacy and property rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt, accurate, and complete notice of the Data Breach.

16. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed Plaintiffs' and Class Members' Private Information. Had Defendant properly monitored its computer network and systems, it could have prevented the

Breach and/or discovered the intrusion sooner to mitigate the injuries to Plaintiffs and the Class.

17. Plaintiffs' and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

18. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

19. Plaintiffs and Class Members may also incur out-of-pocket costs for, *e.g.*, purchasing credit monitoring and identity theft protection services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) actual misuse of the compromised data, including actual and attempted fraud and identity theft and an increase in spam calls, texts, and/or emails; (vi) nominal damages; (vii) emotional distress; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains

backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect their Private Information.

21. Plaintiffs bring this action against Defendant for: (i) negligence and negligence *per se*; (ii) breach of implied contract; (iii) breach of third-party beneficiary contract; (iv) unjust enrichment; (v) violations of Rhode Island's Unfair Trade Practice and Consumer Protection Act, Code of Rhode Island Gen. L. §§ 6-13.1-1 through 6.13.1-11; and (vi) declaratory relief, seeking redress for Deloitte's unlawful conduct.

22. Plaintiffs seek remedies including, but not limited to: compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

23. Plaintiff Ronald J. Pannozzi is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

24. Plaintiff Paola Baldomar is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

25. Plaintiff Meredith Brandt is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

26. Plaintiff Monica Depina is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

27. Plaintiff Meghan Konopka is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

28. Plaintiff Joan Ratcliffe is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

29. Plaintiff Renee Trigueiro is and at all times relevant to this Complaint has been a natural person and individual citizen of the state of Rhode Island.

30. Deloitte Consulting LLP is a Delaware limited liability company with its headquarters and principal place of business located at 30 Rockefeller Plaza, New York, New York 10112. Defendant can be served through its registered agent at: 222 Jefferson Boulevard, Ste. 200, Warick, Rhode Island 02888.

III. JURISDICTION AND VENUE

31. The Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendant.

32. The Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this state; it is registered with the Secretary of State as a foreign registered limited liability company; it maintains an office in Rhode Island; and committed tortious acts in Rhode Island.

33. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Deloitte has the most significant contacts pursuant to the claims of this matter.

IV. STATEMENT OF FACTS

Nature of Defendant's Business

34. Deloitte is a third-party servicer to RIBridges. Deloitte provides "audit and assurance, consulting, tax and related services."[4]

[4] *We're only as good as the good we do*, Deloitte, https://www.deloitte.com/global/en/what-we-do.html?icid=top_what-we-do (last visited Mar. 27, 2025).

35. Deloitte claims that in order to "provide the most impactful services to our clients, we divide our deep subject matter expertise and innovative solutions into six industries and twenty sectors."[5] These industries include: government services, consumer services, financial services, life sciences & healthcare, energy resources, and technology media & communications.

36. Deloitte, in the regular course of its business, collects and maintains the Private Information of state benefit receivers (on behalf of RIBridges) as a requirement of its business practices.

37. Defendant provides data storage services to hundreds of companies worldwide, and claims to securely store data on Defendant's Data Cloud. As a result, Defendant is responsible for developing and maintaining cybersecurity environments which collect and process personal data for their clients and millions of Americans. Defendant touts its ability to do so with its "team of certified privacy professionals bring[ing] dozens of years of experience" to "assist you with data discovery, data posture management, cloud data protection" to "enable[] data privacy and protection across the data lifecycle[.]"[6]

38. Deloitte collected Plaintiffs' and Class Members' Private Information with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

39. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties (including those under a bailment) and knew, or should have known, that it was responsible for protecting Plaintiffs' and

[5] *Industries*, Deloitte, https://www.deloitte.com/global/en/Industries.html (last visited Mar. 27, 2025).

[6] *Cyber & Strategic Risk Solution – Data & Digital Trust*, Deloitte, https://www2.deloitte.com/us/en/pages/risk/solutions/data-and-privacy.html (last visited Mar. 27, 2025)

Class Members' Private Information from unauthorized disclosure.

40. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without that Private Information, Defendant could not have consummated its transactions with RIBridges.

41. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, including, but not limited to: protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

42. Upon information and belief, while collecting the Private Information of Plaintiffs and Class Members, Defendant promised to provide confidentiality and adequate security to protect that highly sensitive data, including in applicable privacy policies and other disclosures in compliance with statutory privacy requirements.

43. Defendant's website explains that: "Data privacy risks have profoundly complicated today's organizations' regulatory, reputational, and operational environments. Our Data Protection and Privacy team delivers practical business solutions that help reduce risk associated with privacy compliance obligations ***and recognize value in personal data***."[7]

44. Defendant's privacy policy explains that Defendant "is a privacy conscious organization."[8] Defendant promises that it has "in place reasonable commercial standards of technology and operational security to protect all personal information . . . from unauthorized access, disclosure, alteration or destruction."[9]

---

[7] *Id.* (emphasis added).
[8] *Privacy Notice*, Deloitte (last revised Nov. 19, 2024), https://www2.deloitte.com/us/en/legal/privacy.html.
[9] *Id.*

45. Deloitte promises in it its Privacy Policy that it is "committed to protecting your privacy."[10]

46. The state of Rhode Island represents that it is committed to protecting the sensitive information of Plaintiffs and Class Members. The state of Rhode Island's privacy policy states: "***We are committed to protecting your privacy online***. When you visit our site, we may collect personal information from you such as your name and e-mail address. ***Our third party hosting company*** will collect additional information such as the URL you came from, your IP address, your domain name, your browser type, the country and state where your server is located, and the pages that were viewed during your visit to our site. ***All this information is kept on a secure server to protect it from outside parties***."[11]

47. Upon information and belief, Deloitte is contractually bound by the obligations and representations of the state of Rhode Island's privacy policy.

48. Upon information and belief, the state of Rhode Island's privacy policy is provided to every applicant, including Plaintiffs and Class Members, upon applying for RIBridges services and state benefits, prior to receiving said services, and upon request.

49. In the course of collecting Private Information from consumers, including Plaintiffs and Class Members, Deloitte promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. Deloitte is aware of and had obligations created by HIPAA, FTCA, contract, industry standards, and state statutory and common law to keep Plaintiffs' and

[10] *Privacy Notice*, Deloitte (last updated June 19, 2024), https://www.deloitte.com/global/en/legal/privacy.html?icid=bn_privacy(.

[11] *Our Privacy Policy*, State of Rhode Island, Executive Office of Health and Human Services, https://eohhs.ri.gov/AboutthisSite/Privacy.aspx (last visited Mar. 27, 2025) (emphasis added).

Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

50. Plaintiffs and Class Members, as consumers, relied on Deloitte's promises and duties to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

51. Consumers, in general, demand that businesses requiring highly sensitive Private Information provide security to safeguard their Private Information, especially when Social Security numbers and PHI are involved.

52. In the course of their dealings, Plaintiffs and Class Members provided Deloitte (through RIBridges) with all or most of the following types of Private Information:

- First and last names;
- Home addresses;
- Dates of birth;
- Financial information;
- HIPAA protected information relating to medical history and health insurance;
- Photo identification and/or driver's licenses;
- Email addresses;
- Phone numbers; and
- Social Security numbers.

53. Deloitte had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties.

The Data Breach

54. According to an online notice published by the state of Rhode Island ("Online Notice"), Deloitte became aware of a cyberattack on its servers on or before December 5, 2024. Deloitte notified the State government of Rhode Island on December 13, 2024 of a "major security threat." As a result, RIBridges systems were suspended and taken offline to address the cyberattack.[12]

55. The Online Notice specifies that an unauthorized actor accessed Deloitte's network sometime around December 5, 2024 and was able to extract certain data from the network. Customers of RIBridges were then unable to access their accounts through their online systems. People applying for benefits with the State could only submit paper applications while the systems were down.

56. Deloitte claimed that "any individual who has received or applied for health coverage and/or health and human services programs or benefits could be impacted by this breach."[13]

57. On January 10, 2025, the state of Rhode Island sent out its Notice of Data Breach Letter to each Plaintiff and Class Member. Upon information and belief, the Notice was adopted by and drafted under the direction and with the agreement of Defendant.[14]

58. The Notice states:

> Your personal information was involved in a recent data breach. This letter tells you about the data breach and what you can do to protect your personal information. Please read this letter carefully. We understand this is a concerning situation, and we thank you for your patience.
>
> **What Happened:** On December 5, 2024, the State was informed by its vendor,

[12] *RI Bridges Alert*, State of Rhode Island, Dep't of Administration, https://admin.ri.gov/ribridges-alert (last visited Mar. 27, 2025).
[13] *Id.*
[14] Accordingly, the Notice will also be referred to as Defendant's Notice.

> Deloitte, that information in the RIBridges system may have been illegally accessed. However, the State and Deloitte took steps right away to address the situation. Federal law enforcement, federal agencies and the Rhode Island State Police were notified. On December 10, 2024, it was confirmed that RIBridges was breached and, on December 11, 2024, that personal information was compromised. When and how the initial access happened are still being investigated. As of now, it is estimated that information of approximately 650,000 people may have been accessed.
>
> **What is RIBridges:** RIBridges is a system that the state of Rhode Island uses to provide benefits, health insurance, and other programs to Rhode Islanders. RIBridges is maintained and operated by Deloitte for the State.
>
> **What Information was Involved in the Data Breach:** The information that may have been exposed includes names, addresses, dates of birth, social security numbers, banking information, telephone number, and health information. The type of information may vary for each individual and program.

59. The Notice lists time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report, freezing their credit, establishing fraud alerts, changing passwords, and notifying law enforcement about suspicious financial account activity. The state of Rhode Island "strongly encourage[d]" Plaintiffs and Class Members to take these steps.

60. State officials separately "urged the thousands of people potentially impacted to freeze their credit, request fraud alerts from their bank, enable multifactor authentication on financial accounts and more."[15]

61. The Governor of Rhode Island separately stated that, "People need to act fast when it comes to protecting their personal information, and for some, that includes keeping an eye on their child's credit[.]"[16]

---

[15] Jonathan Greig, *Rhode Island warns of cybercriminals leaking stolen state files as Deloitte works to restore system*, The Record (Jan. 2, 2025), https://therecord.media/rhode-island-data-breach-deloitte.

[16] *Id.*

62. Defendant, recognizing its fault for the Data Breach, paid $5 million to the state of Rhode Island for expenses related to the December Breach of the RIBridges social services system, including the costs of credit monitoring services offered to victims.[17]

63. Defendant, by way of the state of Rhode Island, merely offered credit monitoring for a limited time in its Notice that Plaintiffs and Class Members could rely on to help mitigate damages. Defendant's offer to provide even these limited services are inadequate as victims will face a risk of identity theft and fraud for their lifetimes. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

64. After RIBridges was taken offline in December 2024, state officials began a phased relaunch of the RIBridges customer portal after a third-party forensics report provided to state officials in January 2025 gave officials enough confidence in the security of the portal to begin a phased relaunch of online services.[18]

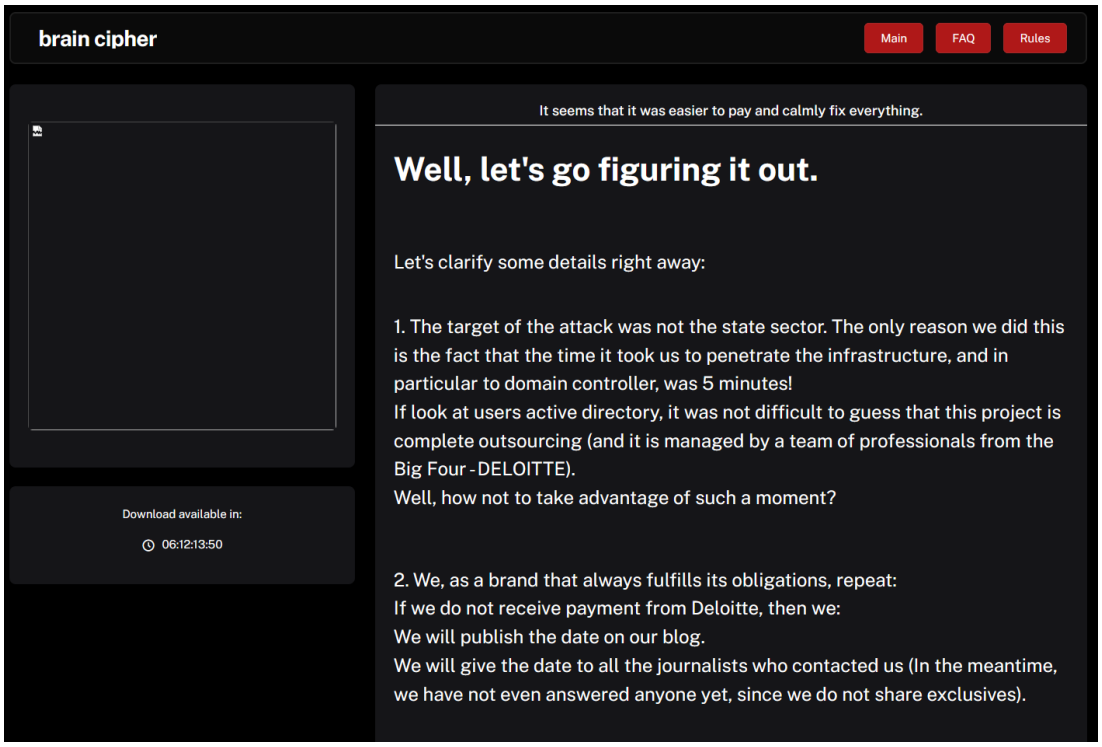
65. In December 2024, a threat group called Brain Cipher claimed credit for the attack against the RIBridges program and sent Deloitte a screenshot containing some of the data they exfiltrated in the Breach, as well as an explanation for the attack and of the weaknesses in Deloitte's cybersecurity:[19]

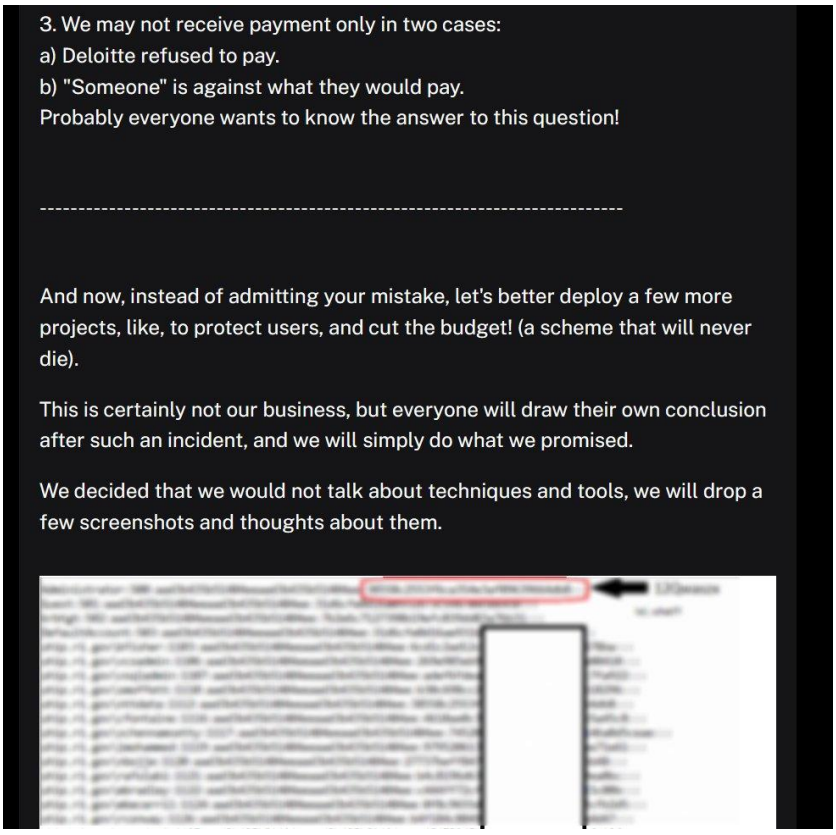
---

[17] David Jones, *Deloitte pays $5M in connection with breach of Rhode Island benefits site*, Cybersecurity Dive (Feb. 5, 2025), https://www.cybersecuritydive.com/news/deloitte-5m-rhode-social-services/739309/.

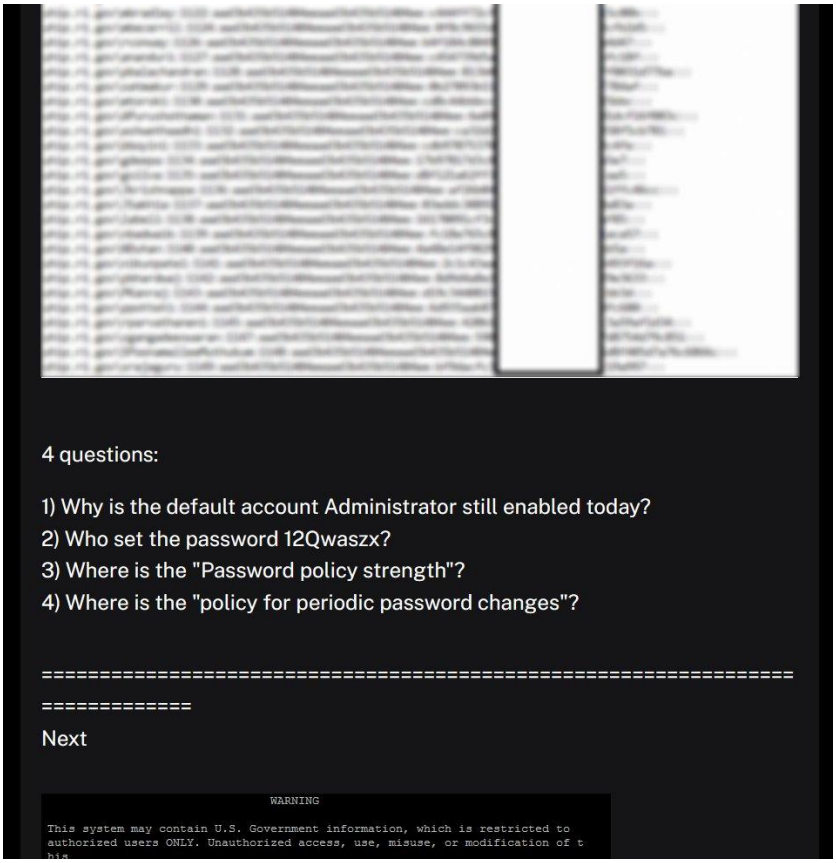
[18] *Id*.

[19] *A Deloitte-Managed State System Getting Jacked By Cybercriminals Will Cost the Firm $5 Million (For Now)*, GoingConcern (Feb. 4, 2025), https://www.goingconcern.com/a-deloitte-managed-state-system-getting-jacked-by-cybercriminals-will-cost-the-firm-5-million-for-now/; https://x.com/DarkWebInformer/status/1871358239822266771 (last visited Mar. 21, 2025).


brain cipher
Main
FAQ
Rules
It seems that it was easier to pay and calmly fix everything.
Well, let's go figuring it out.
Let's clarify some details right away:
1. The target of the attack was not the state sector. The only reason we did this is the fact that the time it took us to penetrate the infrastructure, and in particular to domain controller, was 5 minutes!
If look at users active directory, it was not difficult to guess that this project is complete outsourcing (and it is managed by a team of professionals from the Big Four - DELOITTE).
Well, how not to take advantage of such a moment?
2. We, as a brand that always fulfills its obligations, repeat:
If we do not receive payment from Deloitte, then we:
We will publish the date on our blog.
We will give the date to all the journalists who contacted us (In the meantime, we have not even answered anyone yet, since we do not share exclusives).
Download available in:
06:12:13:50


3. We may not receive payment only in two cases:
a) Deloitte refused to pay.
b) "Someone" is against what they would pay.
Probably everyone wants to know the answer to this question!

And now, instead of admitting your mistake, let's better deploy a few more projects, like, to protect users, and cut the budget! (a scheme that will never die).
This is certainly not our business, but everyone will draw their own conclusion after such an incident, and we will simply do what we promised.
We decided that we would not talk about techniques and tools, we will drop a few screenshots and thoughts about them.



4 questions:

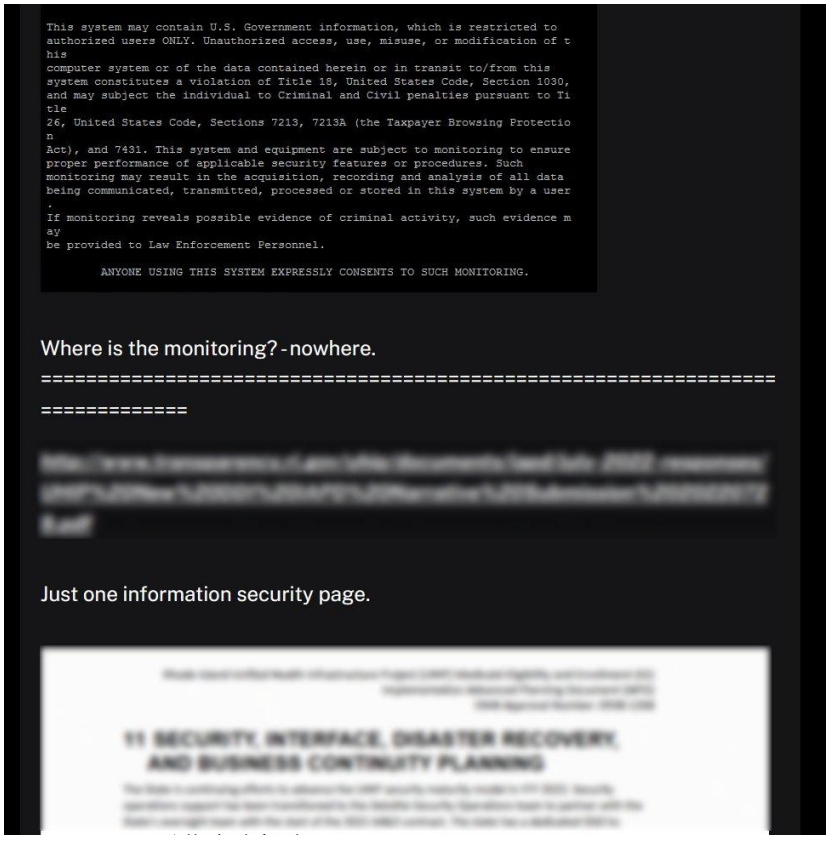
1) Why is the default account Administrator still enabled today?
2) Who set the password 12Qwaszx?
3) Where is the "Password policy strength"?
4) Where is the "policy for periodic password changes"?

==========

Next

WARNING

This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of t
his



This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of t
his
computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Ti
tle
26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protectio
n
Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user
.
If monitoring reveals possible evidence of criminal activity, such evidence m
ay
be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

Where is the monitoring? - nowhere.

==========

Just one information security page.

11 SECURITY, INTERFACE, DISASTER RECOVERY, AND BUSINESS CONTINUITY PLANNING

66. The cybergang suspected to be responsible for the Data Breach—"Brain Cipher"—threatened to release the stolen data to the public via its leak site if Defendant did not pay a ransom.[20] As of December 31, 2024, some of the data was published to the dark web after Defendant refused to pay a ransom.[21] The cybergang claims it stole a total of one terabyte of data,[22] an enormous trove of valuable Private Information.

67. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

68. The Breach was the third reported data breach suffered by the Deloitte brand in 2024.[23] Accordingly, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

69. Deloitte had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties but failed to do so.

70. Upon information and belief, Defendant does not follow its own policies or industry standard practices in securing customers' and employees' Private Information.

71. Upon information and belief, Defendant failed to ensure the proper monitoring and

---

[20] Nish Kohli, *RI Benefits Cyberattack is Still Playing Out. Here's What the State Has Done, and What You Can Do.*, Providence J. (Dec. 17, 2024), https://www.providencejournal.com/story/news/politics/2024/12/17/what-to-know-about-the-ribridges-cyberattack-and-whats-been-done/77050381007.

[21] Andrea Fox, *Brain Cipher begins to leak stolen Rhode Island data*, Healthcare IT News (Dec 31, 2024), https://www.healthcareitnews.com/news/brain-cipher-begins-leak-stolen-rhode-island-data; https://therecord.media/rhode-island-data-breach-deloitte (last visited Mar. 21, 2025).

[22] Mitchell Langley, *Deloitte Hacked: Over 1TB Stolen in Cyberattack*, Sec. Daily Rev. (Dec. 5, 2024), https://dailysecurityreview.com/security-spotlight/deloitte-hacked-over-1tb-stolen-in-cyberattack.

[23] *See* https://www.goingconcern.com/hackers-say-they-got-their-hands-on-deloitte-intranet-communications/ (last visited Mar. 21, 2025); https://www.goingconcern.com/ransomware-gang-says-deloitte-sucks-at-their-job/ (last visited Mar. 21, 2025).

logging of the ingress and egress of network traffic.[24]

72. Upon information and belief, Defendant failed to ensure the proper monitoring and logging of file access and modifications.[25]

73. Upon information and belief, Defendant failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.[26]

74. Upon information and belief, Defendant failed to ensure the proper encryption of Plaintiffs' and Class Members' Private Information and monitor user behavior and activity to identify possible threats.[27]

75. Upon information and belief, Defendant inadequately trains its employees and cybersecurity partners on cybersecurity policies and then fails to enforce those policies.

76. Upon information and belief, Defendant failed to maintain reasonable and adequate security practices over its systems storing Plaintiffs' and Class Members' Private Information.

77. Upon information and belief, Defendant was able to implement reasonable safeguards that would have prevented or mitigated the effects of the Data Breach but failed to do so.[28]

---

[24] https://admin.ri.gov/sites/g/files/xkgbur536/files/2025-01/For-Public-Release-RIBridges-Impacted-Individual-Letter-English.pdf (As of December 5, 2024, Defendant could not determine with certainty whether a breach occurred stating only that the RIBridges system "***may*** have been illegally accessed") (emphasis added).

[25] *Id*.

[26] *Id.* (As of December 10, 2024, Defendant could not determine how the Breach occurred stating only that: "When and how the initial access happened are still being investigated.").

[27] *Id*. (admitting that the Class's "personal information was compromised").

[28] David Jones, *Deloitte pays $5M in connection with breach of Rhode Island benefits site*, Cybersecurity Dive (Feb. 5, 2025), https://www.cybersecuritydive.com/news/deloitte-5m-rhode-social-services/739309/ (in January 2025, less than a month after the Breach, Defendant was able

Plaintiffs' Experience

Plaintiff Ronald J. Pannozzi

78. Plaintiff Pannozzi currently receives benefits from the state of Rhode Island via the RIBridges online portal administered and operated by Defendant.

79. Plaintiff Pannozzi received a Notice letter dated January 10, 2025, informing him that he was a victim of the Breach and that his name, address, date of birth, Social Security number, banking information, telephone number, and health information may have been exposed in the Breach.

80. Plaintiff Pannozzi is very careful about sharing his sensitive Private Information. Plaintiff Pannozzi stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

81. Plaintiff Pannozzi would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

82. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in the Breach has already been misused.

83. Shortly after and as a result of the Breach, Plaintiff Pannozzi began receiving an inordinate amount of spam text messages, emails, and telephone calls from telemarketers. Given the timing of the calls and that they are received on the same number and email that Plaintiff Pannozzi provided to RIBridges, he reasonably believes the calls are related to the Breach. These

---

to make the necessary changes to secure and relaunch the breached portal); *see also* https://x.com/DarkWebInformer/status/1871358239822266771 (the hackers stating that they carried out the Breach because Defendant failed to implement basic security protocols).

calls waste time which cannot be recovered and cause stress to Plaintiff Pannozzi.

84. Prior to the Breach, Plaintiff Pannozzi had never been the victim of fraud or identity theft.

85. As a result of the Breach and following the recommendations in Defendant's Notice letter, Plaintiff Pannozzi has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring his credit reports and financial accounts. Plaintiff Pannozzi has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

86. The Data Breach has caused Plaintiff Pannozzi to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence.

87. As a result of the Data Breach, Plaintiff Pannozzi anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Pannozzi is at a present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

88. Plaintiff Pannozzi has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Paola Baldomar

89. Plaintiff Baldomar currently receives benefits from the state of Rhode Island for herself and her daughter, via the RIBridges online portal administered and operated by Defendant.

90. Plaintiff Baldomar received a Notice letter dated January 10, 2025, informing her that she was a victim of the Breach and that her name, address, date of birth, Social Security

number, banking information, telephone number, and health information may have been exposed in the Breach.

91. Plaintiff Baldomar is very careful about sharing her sensitive Private Information. Plaintiff Baldomar stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

92. Plaintiff Baldomar would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

93. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in the Breach has already been misused.

94. Shortly after (in December of 2024) and as a result of the Data Breach, unauthorized credit inquiries were made on Plaintiff Baldomar's credit for AT&T and a car loan evidencing fraudulent activity.

95. Shortly after and as a result of the Breach, Plaintiff Baldomar learned, in March of 2025, that an unauthorized person claimed Plaintiff Baldomar's two-year-old daughter as a dependent on that unauthorized person's tax return. As a result of this fraudulent activity, Plaintiff Baldomar was forced to spend a significant amount of time filing a police report and talking with the IRS and Social Security administration to correct this fraudulent activity. Plaintiff Baldomar reasonably believes this fraudulent activity is a result of the Breach given the timing, that her daughter is only two-years old, her daughter's father is deceased, and Plaintiff Baldomar has never had this problem before. As a result of this fraudulent activity, Plaintiff Baldomar was unable to efile her tax return and had to spend additional time filing on paper.

96. Prior to the Breach, Plaintiff Baldomar had never been the victim of fraud or

identity theft or (to her knowledge) of another data breach.

97. As a result of the Breach and following the recommendations in Defendant's Notice letter, Plaintiff Baldomar has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her credit reports and financial accounts. Plaintiff Baldomar has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

98. The Data Breach has caused Plaintiff Baldomar to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence which also exposed her minor child's Private Information.

99. As a result of the Data Breach, Plaintiff Baldomar anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Baldomar is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

100. Plaintiff Baldomar has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Meredith Brandt

101. Plaintiff Brandt currently receives benefits from the state of Rhode Island via the RIBridges online portal administered and operated by Defendant.

102. Plaintiff Brandt received a Notice letter dated January 10, 2025, informing her that she was a victim of the Breach and that her name, address, date of birth, Social Security number, banking information, telephone number, and health information may have been exposed in the

Breach.

103. Plaintiff Brandt is very careful about sharing her sensitive Private Information. Plaintiff Brandt stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

104. Plaintiff Brandt would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

105. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in the Breach has already been misused.

106. Shortly after and as a result of the Breach, Plaintiff Brandt received numerous alerts from credit bureaus that her Private Information was published to the dark web.

107. Shortly after and as a result of the Breach, Plaintiff Brandt was advised by her banker that she should open a new account and transfer her funds and automatic payment instructions from her old account to the new one as she had provided RIBridges with all of her banking information when she applied for benefits. These mitigation measures forced Plaintiff Brandt to spend time and energy that she cannot recover.

108. Shortly after and as a result of the Breach, Plaintiff Brandt purchased Turbo Tax ID Notify (identity theft protection), the costs of which were reasonable and necessary. Subsequently, Plaintiff Brandt received an alert from Turbo Tax ID Notify that her Personal Information was published to 12 websites.

109. Prior to the Breach, Plaintiff Brandt had never been the victim of fraud or identity theft or (to her knowledge) of another data breach.

110. As a result of the Breach and following the recommendations in Defendant's Notice

letter, Plaintiff Brandt has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her credit reports and financial accounts, placing fraud alerts on her credit card, and freezing her credit with all three credit bureaus. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

111. The Data Breach has caused Plaintiff Brandt to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence.

112. As a result of the Data Breach, Plaintiff Brandt anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Brandt is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

113. Plaintiff Brandt has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Monica DePina

114. Plaintiff DePina currently receives benefits from the state of Rhode Island for herself and her daughter, via the RIBridges online portal administered and operated by Defendant.

115. Plaintiff DePina received a Notice letter dated January 10, 2025, informing her that she was a victim of the Breach and that her name, address, date of birth, Social Security number, banking information, telephone number, and health information may have been exposed in the Breach.

116. Plaintiff DePina is very careful about sharing her sensitive Private Information.

Plaintiff DePina stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

117. Plaintiff DePina would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

118. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in the Breach has already been misused.

119. Shortly after and as a result of the Breach, Plaintiff DePina began receiving an inordinate amount of harassing and threatening telephone calls from fraudsters attempting to fraudulently obtain funds from Plaintiff. Given the timing of the calls and that they are received on the same number including her husband's telephone number, that Plaintiff DePina provided to RIBridges, she reasonably believes the calls are related to the Breach. These calls waste time which cannot be recovered and cause stress to Plaintiff DePina.

120. In early January of 2025, Plaintiff DePina found that unauthorized charges were made at Amazon.com on her Capital One credit card. As a result of this fraudulent activity, Plaintiff DePina was forced to spend time and energy changing her credit card and disputing the charges. Plaintiff DePina spent several hours dealing with this issue and now checks her accounts several times a days for a total of 15 minutes to a half hour a day.

121. Prior to the Breach, Plaintiff DePina had never been the victim of fraud or (to her knowledge) another data breach.

122. As a result of the Breach and following the recommendations in Defendant's Notice letter, Plaintiff DePina has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her credit reports and financial accounts. Plaintiff DePina

has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

123. The Data Breach has caused Plaintiff DePina to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence which also exposed her minor child's Private Information.

124. As a result of the Data Breach, Plaintiff DePina anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff DePina is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

125. Plaintiff DePina has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Meghan Konopka

126. Plaintiff Konopka currently receives benefits from the state of Rhode Island via the RIBridges online portal administered and operated by Defendant.

127. Plaintiff Konopka received a Notice letter dated January 10, 2025, informing her that she was a victim of the Breach and that her name, address, date of birth, Social Security number, banking information, telephone number, and health information may have been exposed in the Breach.

128. Plaintiff Konopka is very careful about sharing her sensitive Private Information. Plaintiff Konopka stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the

internet or any other unsecured source.

129. Plaintiff Konopka would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

130. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in the Breach has already been misused.

131. Shortly after and as a result of the Breach, Plaintiff Konopka received an alert that her Private Information was published to the dark web.

132. Shortly after and as a result of the Breach, Plaintiff Konopka received an alert in January of 2025 that her debit card had been used fraudulently. Due to this fraud, Plaintiff Konopka was forced to spend two hours resolving this issue with her bank. Plaintiff Konopka never had this issue prior to the Breach and reasonably believes this fraud is a result of the Breach.

133. Shortly after and as a result of the Breach, Plaintiff Konopka began receiving an inordinate amount of spam and harassing telephone calls from telemarketers (approximately ten a day). Given the timing of the calls and that they are received on the same number that Plaintiff Konopka provided to RIBridges, she reasonably believes the calls are related to the Breach. These calls waste time which cannot be recovered and cause stress to Plaintiff Konopka.

134. As a result of the Breach and following the recommendations in Defendant's Notice letter, Plaintiff Konopka has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her credit reports and financial accounts. Plaintiff Konopka has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

135. The Data Breach has caused Plaintiff Konopka to suffer fear, anxiety, and stress,

which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence.

136. As a result of the Data Breach, Plaintiff Konopka anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Konopka is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

137. Plaintiff Konopka has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Joan Ratcliffe

138. Plaintiff Ratcliffe currently receives benefits from the state of Rhode Island via the RIBridges online portal administered and operated by Defendant.

139. Plaintiff Ratcliffe received a Notice letter dated January 10, 2025, informing her that she was a victim of the Breach and that her name, address, date of birth, Social Security number, banking information, telephone number, and health information may have been exposed in the Breach.

140. Plaintiff Ratcliffe is very careful about sharing her sensitive Private Information. Plaintiff Ratcliffe stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

141. Plaintiff Ratcliffe would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

142. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in

the Breach has already been misused.

143. Shortly after and as a result of the Data Breach, Plaintiff Ratcliffe was alerted by her bank on December 19, 2024 that unauthorized individuals were attempting to transfer money out of her bank account. The hackers had already uploaded email accounts to which they intended to transfer money when Plaintiff Ratcliffe with the help of a bank representative froze her account. This fraudulent activity caused Plaintiff Ratcliffe to spend time and energy, including to open up a new bank account in person and transfer funds and automatic payment and deposit instructions from the old to the new account, time that cannot be recovered.

144. Shortly after and as a result of the Data Breach, Plaintiff Ratcliffe purchased Equifax credit monitoring, the cost of which was reasonable and necessary.

145. Prior to the Breach, Plaintiff Ratcliffe had never been informed that she was a victim of a data breach.

146. As a result of the Breach and following the recommendations in Defendant's Notice letter, Plaintiff Ratcliffe has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her credit reports and financial accounts. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

147. The Data Breach has caused Plaintiff Ratcliffe to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff Ratcliffe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Ratcliffe is at a present risk and will continue to

be at increased risk of identity theft and fraud for her lifetime.

149. Plaintiff Ratcliffe has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Renee Trigueiro

150. Plaintiff Trigueiro currently receives benefits from the state of Rhode Island for herself and her five children, via the RIBridges online portal administered and operated by Defendant.

151. Plaintiff Trigueiro received a Notice letter dated January 10, 2025, informing her that she was a victim of the Breach and that her name, address, date of birth, Social Security number, banking information, telephone number, and health information may have been exposed in the Breach.

152. Plaintiff Trigueiro is very careful about sharing her sensitive Private Information. Plaintiff Trigueiro stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

153. Plaintiff Trigueiro would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

154. As described *infra*, the data set obtained in the Data Breach was published to the dark web by the hacker group Brain Cipher, demonstrating that the Private Information stolen in the Breach has already been misused.

155. Shortly after and as a result of the Breach, Plaintiff Trigueiro received an alert from Credit Karma on December 17, 2024 that an unauthorized individual had opened a Chime account in her name. Credit Karma later informed her that the unauthorized Chime account was listed on

her credit report in error.

156. Shortly after and as a result of the Breach, Plaintiff Trigueiro learned that an unauthorized individual attempted to use her EBT card in early January of 2025. Plaintiff Trigueiro noticed the fraudulent transactions herself as she has been monitoring her EBT account daily since learning of the Breach. After seeing the fraudulent transactions, Plaintiff Trigueiro locked her EBT card. She keeps the card locked but has to unlock the card every time she needs to use it. This fraudulent activity has caused Plaintiff Trigueiro to spend valuable time and energy that she cannot recover.

157. Prior to the Breach, Plaintiff Trigueiro had never been the victim of identity theft or fraud.

158. As a result of the Breach and following the recommendations in Defendant's Notice letter, Plaintiff Trigueiro has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, monitoring her credit reports and financial accounts for 30 minutes every day. Plaintiff Trigueiro has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

159. The Data Breach has caused Plaintiff Trigueiro to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not informed Plaintiff of key details about the Data Breach's occurrence, which also exposed her minor children's Private Information.

160. As a result of the Data Breach, Plaintiff Trigueiro anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Trigueiro is at a present risk and will continue to be at increased risk of identity theft and fraud for her lifetime.

161. Plaintiff Trigueiro has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

162. It is well known that Private Information, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Deloitte, are well aware of the risk of being targeted by cybercriminals.

163. Individuals place a high value not only on their Private Information, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

164. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[29]

165. Individuals, like Plaintiffs and Class members, are particularly concerned with

[29] *Victims of Identity Theft, 2018*, U.S. Department of Justice (April 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

166. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

167. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[30]

168. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[31]

169. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from

[30] *Identity Theft and Your Social Security Number*, SSA.gov, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 5, 2024).

[31] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited Dec. 5, 2024).

"misconfigurations, human error, poor maintenance, and unknown assets."[32]

170. Indeed, 2023 represented an all-time high for data breaches, with 3,205 breaches affecting 353,027,892 total victims. The estimated number of organizations impacted by data breaches has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 breaches represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of breaches (1,860) set in 2021.

171. In light of recent high profile data breaches across industries in the years, including T-Mobile, USA (37 million records, February-March 2023), and NCB Management Services, Inc. (1 million records, February 2023), and affecting healthcare entities and partners in recent years, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

172. Cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware

[32] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[33]

173. Indeed, the Breach was the third reported data breach suffered by the Deloitte brand in 2024.[34]

174. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, Deloitte failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times, Defendant Had a Duty to Plaintiffs and Class Members to Properly Secure their Private Information

175. At all relevant times, Deloitte had a duty to Plaintiffs and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when Deloitte became aware that their Private Information was compromised.

176. Defendant had the resources necessary to prevent the Data Breach but neglected to

[33] Ben Kochman, *FBI, Secret Service Warn Of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

[34] *See Hackers Say They Got Their Hands on Deloitte Intranet Communications*, GoingConcern (Sept. 25, 2024), https://www.goingconcern.com/hackers-say-they-got-their-hands-on-deloitte-intranet-communications/; *Ransomware Gang Says Deloitte Sucks at Their Job*, GoingConcern (Dec. 11, 2024),https://www.goingconcern.com/ransomware-gang-says-deloitte-sucks-at-their-job/.

adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

177. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;
b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
c. Monitoring for suspicious or irregular traffic to servers;
d. Monitoring for suspicious credentials used to access servers;
e. Monitoring for suspicious or irregular activity by known users;
f. Monitoring for suspicious or unknown users;
g. Monitoring for suspicious or irregular server requests;
h. Monitoring for server requests for Private Information;
i. Monitoring for server requests from VPNs; and
j. Monitoring for server requests from Tor exit nodes.

178. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[35] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[36]

179. The ramifications of Defendant's failure to keep consumers' Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims including Plaintiffs and the Class may continue for years.

180. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[37] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed[,] 69 percent reported feelings of fear related to personal financial safety[,] 60 percent reported anxiety[,] 42 percent reported fearing for the financial security of family members[, and] 8 percent reported feeling suicidal."[38]

The Value of Personal Identifiable Information

181. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[39]

182. Criminals can also purchase access to entire company's data breaches from $900

[36] *Id*.
[37] Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, NortonLifeLock (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft?srsltid=AfmBOorWguVbuVLpKXO6-0gKBs87unsFhintKF98izq0DAv1Xpve5WAX.
[38] *Id.*
[39] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

to $4,500.[40]

183. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[41]

184. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

185. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[42]

---

[40] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[41] *Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 5, 2024).

[42] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

186. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[43]

187. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[44]

188. Given the nature of this Data Breach, it is foreseeable that the compromised Private Information can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' Private Information can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

189. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

190. Moreover, Deloitte is offering a limited time offer for identity theft monitoring and identity theft protection. Its limitation is inadequate when victims are likely to face many years of identity theft.

191. Furthermore, Defendant's credit monitoring offer and advice to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words,

[43] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[44] *See* Office of Mgmt. & Budget, OMB Memorandum M-07-16 at n.1 (last visited Dec. 5, 2024).

Defendant expects Plaintiffs and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

192. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

193. The injuries to Plaintiffs and Class Members were directly and proximately caused by Deloitte's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

194. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[45]

195. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

[45] *Start With Security*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 5, 2024).

practices for business.[46] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

196. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[47]

197. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[48]

198. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system

[46] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Dec. 5, 2024).

[47] *Data Breach Response: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last visited Dec. 5, 2024).

[48] *See* FTC, *Start With Security*, *supra*.

and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user.

> If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

199. The FTC has brought enforcement actions against businesses for failing to protect consumers and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

200. Because Plaintiffs and Class Members entrusted Defendant with their Private Information, Defendant had, and has, a duty to the Plaintiffs and Class Members to keep their Private Information secure.

201. Plaintiffs and the other Class Members reasonably expected that when they provide Private Information to Defendant (or to RIBridges), Defendant would safeguard their Private Information.

202. Deloitte was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiffs and members of the Class. Deloitte was also aware of the significant repercussions if it failed to do so. Its own Privacy Policies, quoted above, acknowledge this awareness.

203. Deloitte's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Concrete Injuries are Caused by Defendant's Inadequate Security.

204. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

205. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. Plaintiffs and other individuals whose Private Information was entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

206. Cybercriminals intentionally attack and exfiltrate Private Information to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

207. The cybercriminals who obtained the Class Members' Private Information may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other Private Information, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;

- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

208. Upon Information and belief, Class Members' Private Information has and/or will be published for sale on the Dark Web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyberattacks of this type.

209. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

210. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their Private Information, for which there is a well-established national and international market.

211. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

212. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers

at a substantial risk of fraud."[49] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

213. As a result of the Data Breach, Plaintiffs and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

Data Breaches Put Consumers at an Increased Risk of Fraud and Identify Theft.

214. Data Breaches such as the one experienced Plaintiffs and Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

215. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[50] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiffs and Class Members) must take after a breach like Defendant's are both time-consuming and of limited and short-term effectiveness.

216. The FTC, like the GAO, recommends that identity theft victims take several steps

[49] *The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas*, https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf (last visited Dec. 5, 2024).

[50] U.S. Gov't Accountability Off., GAO-19-230, *Report to Congressional Requestors: Range of Consumer Risks Highlights Limitations of Identify Theft Services* (Mar. 2019), https://www.gao.gov/assets/gao-19-230.pdf.

to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[51]

217. Theft of Private Information is also gravely serious. Private Information is a valuable property right.[52]

218. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

219. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for their lifetimes.

220. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a

[51] *See What To Do Right Away*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Mar. 27, 2025).

[52] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

PHI record at $1000 each."[53]

CLASS ACTION ALLEGATIONS

221. Plaintiffs bring this action individually and on behalf of all other persons similarly situated.

222. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach that occurred at Defendant on or about December 5, 2024 (the "Class").

223. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

224. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

225. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 700,000 persons whose data was compromised in Data Breach.

226. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

---

[53] *A Cost Analysis of Healthcare Sector Data Breaches*, HHS, https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last visited Jan. 19, 2023).

A. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

B. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

C. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

D. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

E. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

F. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

G. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

H. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

I. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

J. Whether Defendant's conduct was negligent;

K. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

L. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

227. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

228. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

229. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

230. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

231. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-

wide basis. Further, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, is encrypted, and is password protected. Damages from a future breach due to Defendant's inadequate data security represent an irreparable injury (such as the further loss of privacy and exposure of Private Information such as Social Security numbers) for which no adequate remedy at law exists.

232. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

A. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

B. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

C. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

D. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

E. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

233. Finally, all members of the proposed Class are readily ascertainable. Defendant has

access to Class Members' names and addresses. Class Members have already been preliminarily identified and sent notice of the Data Breach by Deloitte.

CAUSES OF ACTION

FIRST COUNT
Negligence and Negligence *Per Se*
(On behalf of Plaintiffs and All Class Members)

234. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

235. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of the regular course of its business operations. Plaintiffs and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

236. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

237. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

238. Defendant had a duty to employ reasonable security measures under Section 5 of

the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

239. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

240. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

241. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

242. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

243. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

244. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who received its services, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

245. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

246. Plaintiffs and Class Members are within the class of persons that HIPAA is intended to protect.

247. The harms that Plaintiffs and Class Members suffered as a result of the Breach are within the scope of harms that HIPAA is intended to protect against.

248. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

249. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

250. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

251. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their Private Information that was in Defendant's possession.

252. Defendant had a special relationship with Plaintiffs and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiffs and Class Members by ensuring that their personal information would remain

protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiffs' and Class Members' Private Information. The harm to Plaintiffs and Class members from its exposure was highly foreseeable to Defendant.

253. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

254. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

255. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

256. Defendant alone was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

257. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their Private Information.

258. Defendant's willful failure to abide by these duties was wrongful, reckless, and

grossly negligent in light of the foreseeable risks and known threats.

259. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

260. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

261. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

262. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

263. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

264. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

265. Plaintiffs and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

266. Plaintiffs re-allege and incorporate by the paragraphs above as if fully set forth herein.

267. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving services provided by Defendant.

268. Plaintiffs and Class Members provided their Private Information to Defendant or its third-party agents in exchange for Deloitte's services. In exchange for the Private Information, Defendant promised to protect their Private Information from unauthorized disclosure.

269. At all relevant times Defendant promulgated, adopted, and/or implemented a written Privacy Policy and HIPAA Notice whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

270. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

271. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information, was Defendant's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

272. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

273. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

274. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

275. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

276. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

277. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

278. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

279. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

280. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

281. Plaintiffs and Class Members are also entitled to injunctive relief requiring

Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

THIRD COUNT
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and All Class Members)

282. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

283. Plaintiffs and Class Members provided their Private Information to Defendant as part of receiving benefits and services through the RIBridges portal.

284. Defendant was responsible for managing and operating the RIBridges portal, via contracts with the state of Rhode Island.

285. Those contracts were made expressly for the benefit of Plaintiffs and Class Members, whose Private Information Defendant collected, stored, and maintained, in order to operate and administer the RIBridges portal consistent with its contractual obligations with the state of Rhode Island.

286. Plaintiffs and Class Members were the intended beneficiaries of the contracts entered into by Defendant and the state of Rhode Island—there would be no need for Defendant's services aside from the benefit to Plaintiffs and Class Members. The contracts between Defendant and the state of Rhode Island were therefore clearly intended for the benefit of Plaintiffs and Class Members, and the benefits of those contracts were directed at Plaintiffs and Class Members.

287. That Plaintiffs and Class Members would rely on the contracts between Defendant and the state of Rhode Island to ensure the security of their Private Information was foreseeable to Defendant.

288. Defendant breached its contracts with the state of Rhode Island when it failed to use reasonable data security measures to adequately protect Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure.

289. Plaintiffs and Class Members were foreseeably harmed by Defendant's failure to use reasonable data security measures, as alleged herein.

290. Accordingly, Plaintiffs and Class Members are entitled to compensatory, nominal, and consequential damages suffered as a result of the Data Breach.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

291. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

292. Plaintiffs and Class Members conferred a benefit on Defendant in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

293. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

294. Acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over

the requisite data security.

295. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

296. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

297. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

298. Plaintiffs and Class Members have no adequate remedy at law.

299. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

300. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class

Members have suffered and will continue to suffer other forms of injury and/or harm.

301. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FIFTH COUNT
Violation of Rhode Island's Unfair Trade Practice and Consumer Protection Act
Code of Rhode Island Gen. L. §§ 6-13.1-1 through 6.13.1-11
(On Behalf of Plaintiffs and All Class Members)

302. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

303. Defendant is a "person" as defined by R.I. Gen. L. § 6-13.1-1(3).

304. Defendant violated R.I. Gen. L. 6-13.1-11 ("UTPCPA") by engaging in unlawful and unfair or deceptive business acts and practices.

305. The acts and omissions complained of herein were designed in and emanated from this District.

306. Defendant's "unfair" acts and practices include:

a. utilizing cheaper, ineffective security measures and diverting those funds to their own profits, instead of providing a reasonable level of security that would have prevented the Data Breach;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information.

307. Defendant has engaged in unlawful business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and Rhode Island common law.

308. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

309. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of Plaintiffs' and Class Members' Private Information.

310. As a direct and proximate result of Defendant's unfair and unlawful acts and practices, Plaintiffs and Class Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

311. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

312. Plaintiffs and Class Members would not have engaged with Defendant's business, had they known that Defendant failed to employ appropriate measures to secure Plaintiffs' and Class Members' Private Information.

313. Plaintiffs and Class Members have lost money and property as a result of Defendant's conduct in violation of the UTPCPA, as stated herein and above.

314. By deceptively storing, collecting, and disclosing their Private Information, Defendant has taken money or property from Plaintiffs and Class Members.

315. Defendant acted intentionally, knowingly, and maliciously to violate Rhode Island's UTPCPA, and recklessly disregarded Plaintiffs' and Class Members' rights.

316. Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair and unlawful business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

SIXTH COUNT
Declaratory Judgment
(On Behalf of Plaintiffs and All Class Members)

317. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

318. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

319. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information.

320. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

321. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Deloitte continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various state statutes; and

b. Deloitte continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

322. The Court also should issue corresponding prospective injunctive relief requiring Deloitte to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

323. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Deloitte. The risk of another such breach is real, immediate, and substantial. If another breach at Deloitte occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

324. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Deloitte if an injunction is issued. Among other things, if another massive data breach occurs at Deloitte, Plaintiffs and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Deloitte of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Deloitte has a pre-existing legal obligation to employ such measures.

325. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Deloitte, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, punitive, nominal, and statutory damages, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: March 28, 2025

Respectfully submitted,

/s/ Danielle L. Perry
Gary E. Mason*
Danielle L. Perry*

Lisa A. White*
MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Fax: (954) 525-4300
Email: ostrow@kolawyers.com

Interim Co-Lead Class Counsel

Vincent L. Greene
MOTLEY RICE LLC
40 Westminster St., 5th Floor
Providence, RI 02903
Telephone: (401) 457-7700
Fax: (401) 457-7708
Email: vgreene@motleyrice.com

Local Liaison Counsel

Peter N. Wasylyk (RI Bar No. 3351)
LAW OFFICES OF PETER N. WASYLYK
1307 Chalkstone Ave.
Providence, RI 02908
Telephone: (401) 831-7730
Fax: (401) 861-6064
Email: pnwlaw@aol.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Email: gklinger@milberg.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, L.P.A.

4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Telephone: (513) 345-8297
Email: jgoldenberg@gs-legal.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN
COUNSELORS AT LAW
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Email: cschaffer@lfsblaw.com

Daniel Srourian*
SROURIAN LAW FIRM, P.C.
468 N. Camden Dr. Suite 200
Beverly Hills, CA 90210
Telephone: (213) 474-3800
Fax: (213) 471-4160
Email: daniel@slfla.com

Lynda J. Grant*
THEGRANTLAWFIRM, PLLC
521 Fifth Avenue, 17th Floor
New York, NY 10175
Telephone: (212) 292-4441
Fax: (212) 292-4442
Email: lgrant@grantfirm.com

Gary S. Graifman*
Melissa R. Emert*
KANTROWITZ, GOLDHAMER &
GRAIFMAN, P.C.
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Telephone: (201) 391-7000
Fax: (201) 307-1086
Email: ggraifman@kgglaw.com
Email: memert@kgglaw.com

J. Gerard Stranch, IV*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Ste 200
Nashville, TN 37203
Telephone: (615) 254-8801

Email: gstranch@stranchlaw.com
Email: gwells@stranchlaw.com

James J. Pizzirusso*
Amanda V. Boltax*
Nicholas Murphy*
Ashley M. Crooks*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
Fax: (202) 540-7201
Email: jpizzirusso@hausfeld.com
Email: mboltax@hausfeld.com
Email: nmurphy@hausfeld.com

Executive Committee

**pro hac vice or applications for admission to be filed*